

Seguridad de la Información
en Ecuador 2017

Estudio 2017
Deloitte Ecuador

Índice



Introducción

Deloitte presenta la **primera edición** de su estudio de Seguridad de la Información - Ecuador 2017, en el cual se miden las principales tendencias en cuanto a seguridad de la información así como sus retos y obstáculos.

El estudio realizado por Deloitte tiene como objetivo **ser una herramienta de comparación que permita a las organizaciones mejorar los aspectos estratégicos, tácticos y operativos en cuanto a la gestión de seguridad de la información.**

Participaron más de 50 empresas nacionales y multinacionales de diversas industrias.



Detalle de participantes

Distintos sectores e industrias



Región a la que pertenecen las organizaciones



Cantidad de empleados en la organización

19%
Hasta 200

23%
Entre 200 y 500

19%
Entre 500 y 1000

23%
Entre 1000 y 5000

16%
Más de 5000

Principales Tendencias



Casi el **50% de participantes** sufrieron alguna brecha de seguridad en los últimos 12 meses, y de estos, el **20%** no pudo determinar el impacto de dicha brecha ya que no cuentan con un proceso de gestión de incidentes.





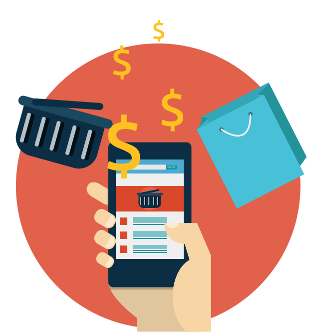
El componente humano continua siendo una pieza crítica en la gestión de seguridad de la información, lo cual es confirmado por casi el **50% de los participantes** que indicaron que su principal iniciativa para el 2018 será la capacitación y sensibilización en seguridad de la información. La gran mayoría de iniciativas recae en el ámbito estratégico y táctico.



Principales Tendencias



La falta de suficiente presupuesto continua estando entre las principales dificultades, lo cual es confirmado por más del **50% de los participantes,** seguido muy de cerca por aspectos como la falta de visibilidad e influencia y la falta de personal competente. Así mismo, casi el **75% de los participantes** no mide el retorno de las inversiones en seguridad de información.



Solo el 20% está preparado para afrontar incidentes de seguridad originados en redes sociales.

El **60% de los participantes** no disponen actualmente de un SOC, pero **casi el 20%** afirma que contará con uno para el 2018.



Principales Tendencias

Deloitte cuenta con un enfoque basado en buenas prácticas y que cubre los componentes básicos: asegurar, detectar y responder.



Se enfoca en la protección de la información que soporta los procesos claves del negocio, implementando procesos y controles que responden a la realidad y circunstancias del mismo.



Reconoce la necesidad de establecer una cultura proactiva de estar atentos a las amenazas a fin de desarrollar una capacidad de detectar patrones de comportamiento que puedan indicar o predecir un ataque a la información crítica.



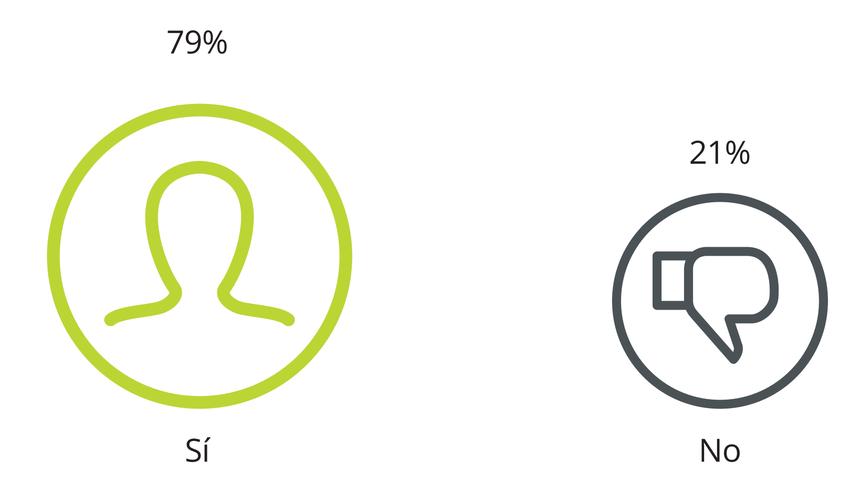
Significa tener la capacidad de controlar rápidamente un ataque y movilizar los recursos necesarios para manejar el impacto, incluyendo costos directos y disrupción del negocio, así como también daños a la reputación y marca.

Seguro



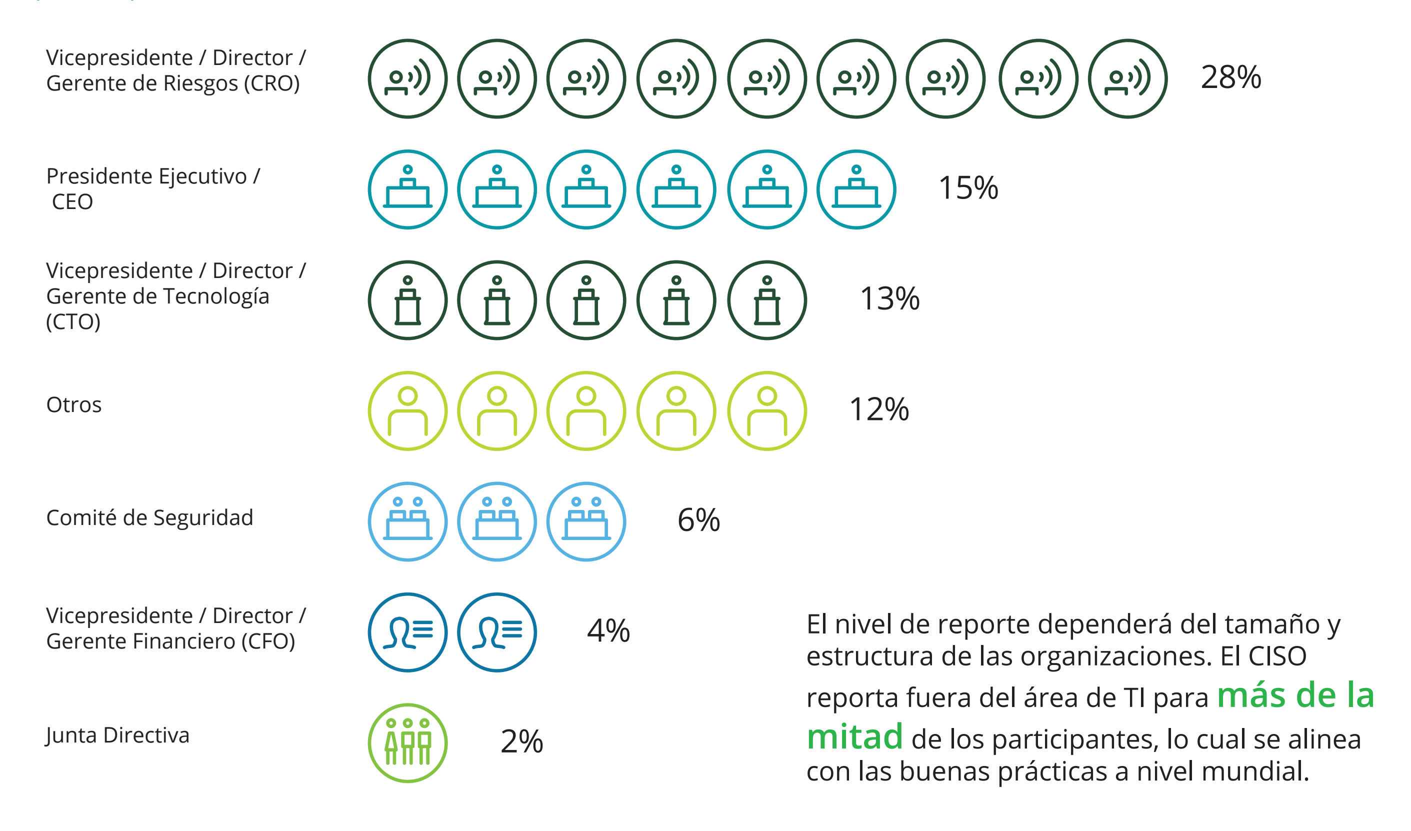
Responsable de seguridad de la información y nivel de reporte

¿Cuenta su organización con un responsable de seguridad de la información (CISO – Chief Information Security Officer) o similar?



En Ecuador, la función de seguridad de la información se encuentra consolidada dado que **8 de cada 10** participantes cuenta con un CISO formal.

¿A quién reporta el CISO?



El nivel de reporte dependerá del tamaño y estructura de las organizaciones. El CISO reporta fuera del área de TI para **más de la mitad** de los participantes, lo cual se alinea con las buenas prácticas a nivel mundial.

Responsabilidades del CISO

¿Qué áreas y/o funciones de seguridad de la información (SI) se encuentran bajo responsabilidad del CISO?

Gobierno de SI (políticas, normas, estándares)



Monitoreo de SI (Indicadores, métricas y reportes)



Cumplimiento y control de SI



Concientización y capacitación en SI



Administración de usuarios y accesos



Administración del riesgo de TI / SI



Respuesta ante incidentes de SI



Estrategia, planificación y presupuesto de SI



Monitoreo de eventos de SI, marcas y riesgos externos (ciber-inteligencia)

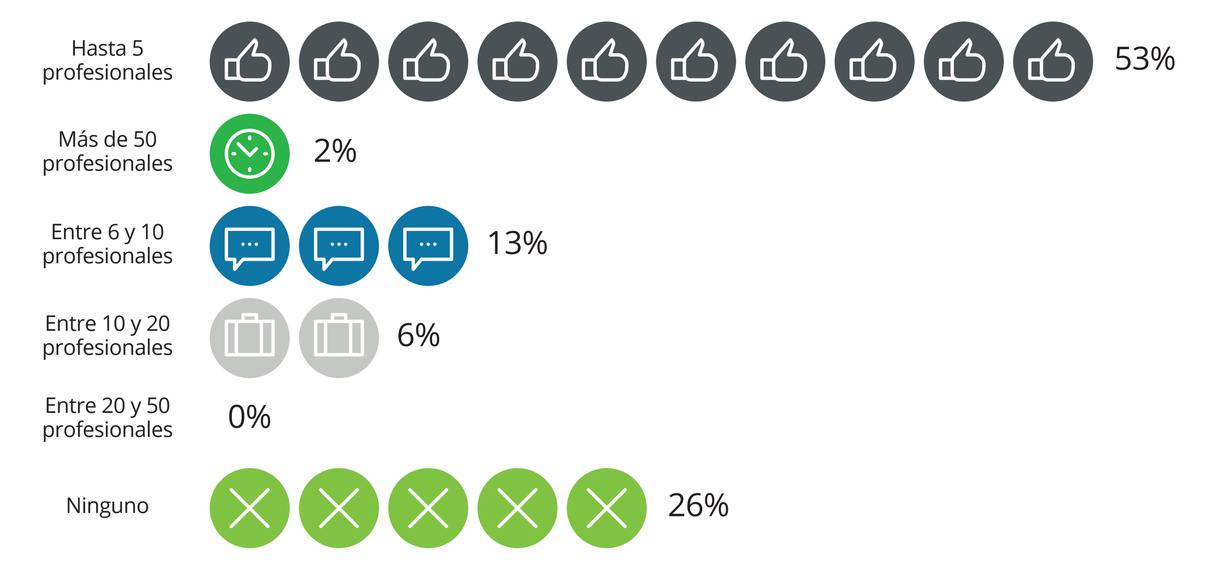


El CISO gestiona áreas o funciones consistentes con las buenas prácticas, entre las más destacadas tenemos: **Gobierno de SI, Monitoreo de SI y Cumplimiento de SI, Sensibilización, Respuesta ante Incidentes;** lo cual es corroborado por las **tres cuartas partes** de los encuestados. Existen otras responsabilidades como: Seguridad de las aplicaciones y datos, Administración de vulnerabilidades, Arquitectura de SI, Operaciones de SI, Seguridad de terceras partes y socios de negocio, Plan de recuperación ante desastres, Administración de continuidad del negocio, Seguridad física, que también fueron nombradas en el estudio.

Funciones como Seguridad física y Administración de continuidad de negocio no forman parte de las responsabilidades del CISO, a pesar de que estas áreas guardan relación con la seguridad de información a través del atributo "Disponibilidad".

Profesionales en seguridad de la información

¿Cuántos profesionales dedicados a tiempo completo a la seguridad de información (SI) tiene su organización?



No existe una cantidad correcta de recursos, dependerá de aspectos como: tamaño de la organización, regulaciones de la industria y actividades asignadas al área de SI. **La mitad de los participantes dispone de hasta 5 profesionales dedicados a tiempo completo.** Aún existen empresas que no cuentan con profesionales dedicados a la SI exclusivamente.

Principales obstáculos

¿Cuáles son los principales obstáculos que enfrenta para desarrollar la estrategia y programa de seguridad de información efectivo?

Luego de los ataques mundiales e incidentes de seguridad propios, las empresas se han dado cuenta que requieren invertir más en capacitar sus recursos, en temas de seguridad de información.

La **mitad de los participantes** consideran que no cuentan con los suficientes recursos para su gestión así como carecen visiblidad e influencia dentro de la organización. Este aspecto puede responder a situaciones como: el enfoque de riesgos aplicado, el nivel de sensibilización de los tomadores de decisión, y factores externos como la economía, lo cual generó limitaciones en la inversión de las organizaciones a nivel local.

55%



Falta de suficiente presupuesto y/o recursos

42%



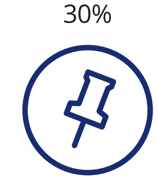
Falta de visibilidad e influencia dentro de la organización

34%



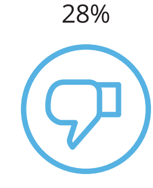
Falta de recursos capacitados y competentes en el mercado

30%



Falta de claridad sobre el ámbito de gestión, funciones y responsabilidades

28%



Falta de apoyo ejecutivo o del negocio

26%



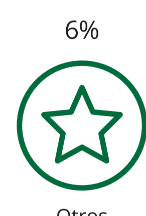
Falta de una estrategia de seguridad de la información y hoja de ruta de implementación

19%



El impacto de las nuevas tecnologías y/o amenazas

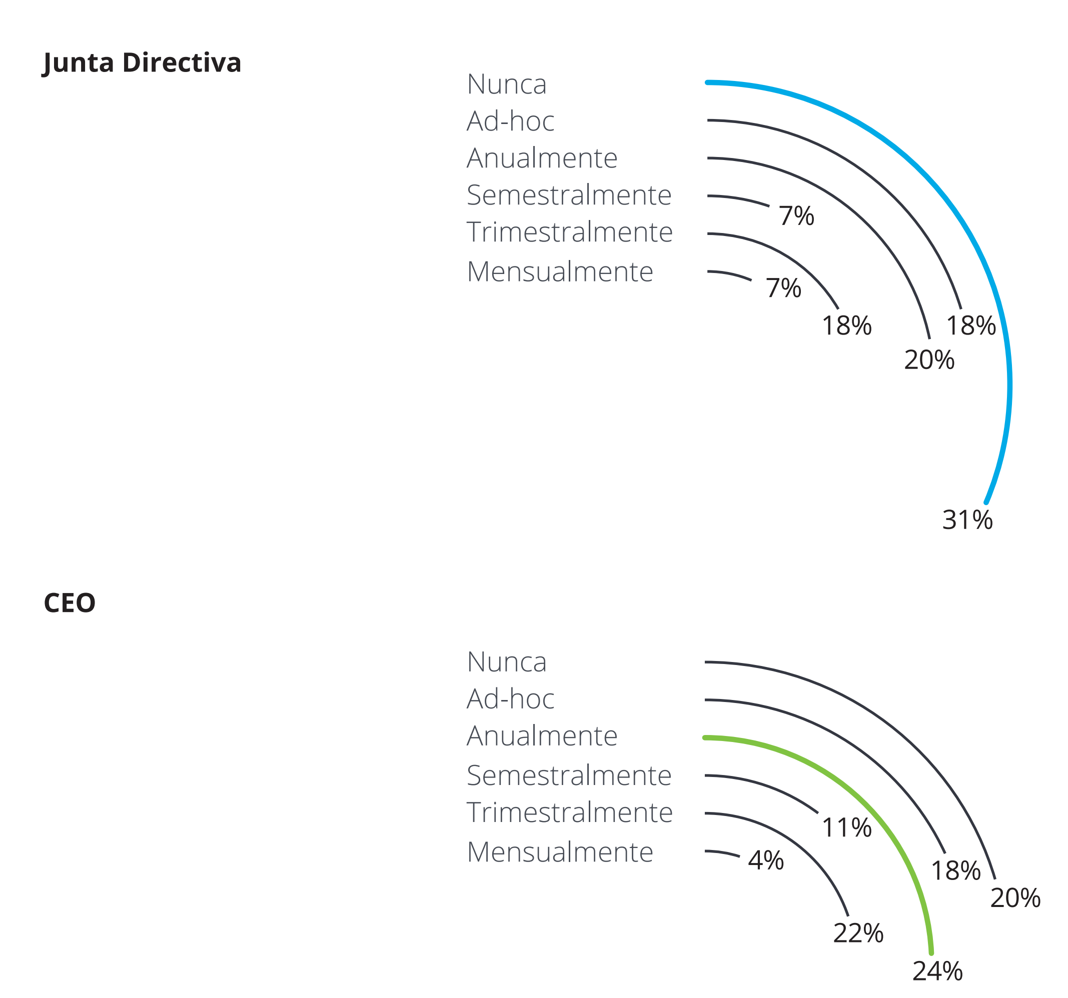
6%



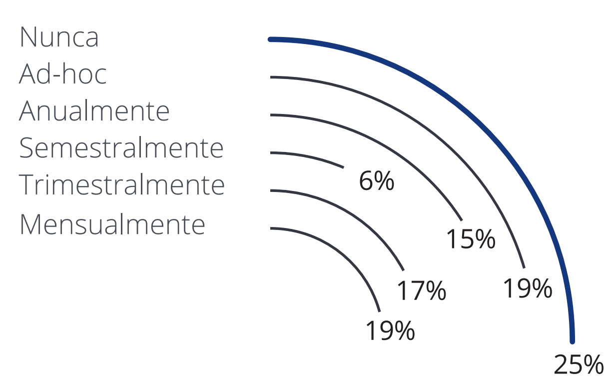
Otros

Frecuencia de reporte

¿Con qué frecuencia se reporta sobre la situación de seguridad de la información a las principales autoridades de su organización?



Alta Dirección y/o Comité Ejecutivo



Más de la mitad de los participantes mantienen un nivel de comunicación proactivo con los altos ejecutivos sobre la gestión de la seguridad de la información. Es importante recalcar que se debe contar con un mecanismo formal y proactivo, que no sólo transmita brechas de seguridad, sino también cómo evoluciona la gestión de seguridad en la organización.

Monitoreo de la gestión de seguridad de la información

Describa su enfoque hacia el monitoreo de la gestión de seguridad de la información

36%



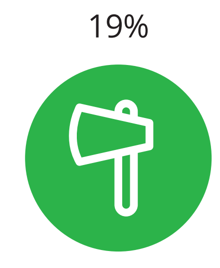
No se cuenta con un enfoque de monitoreo de seguridad de información.

30%



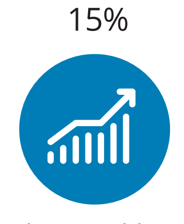
Se cuenta con métricas de SI que permiten comprender mejor el proceso así como fortalezas y necesidades

19%



Se cuenta con un esquema de medición (métricas operacionales) pero se mide bajo demanda / necesidad.

15%



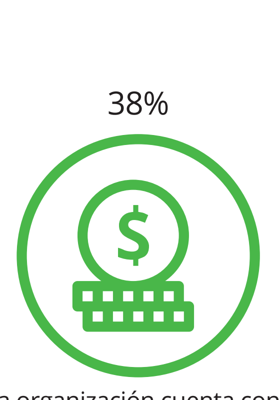
Se han establecido Indicadores Claves del Proceso (KPI) y Indicadores Claves de Riesgo (KRI) de SI

Más de la mitad de participantes realizan algún tipo de monitoreo de aspectos relacionados con seguridad de información, lo cual permite interactuar con el negocio y presentar resultados de la gestión realizada. Así mismo, aún no existe una comprensión clara de la importancia de este proceso dado que **1 de 3 participantes** no realizan ningún tipo de monitoreo.

Presupuesto para la gestión de seguridad de la información

¿Su organización cuenta con un presupuesto específico aplicado a la gestión de seguridad de la información?

38%



Si, la organización cuenta con un presupuesto definido para SI

62%

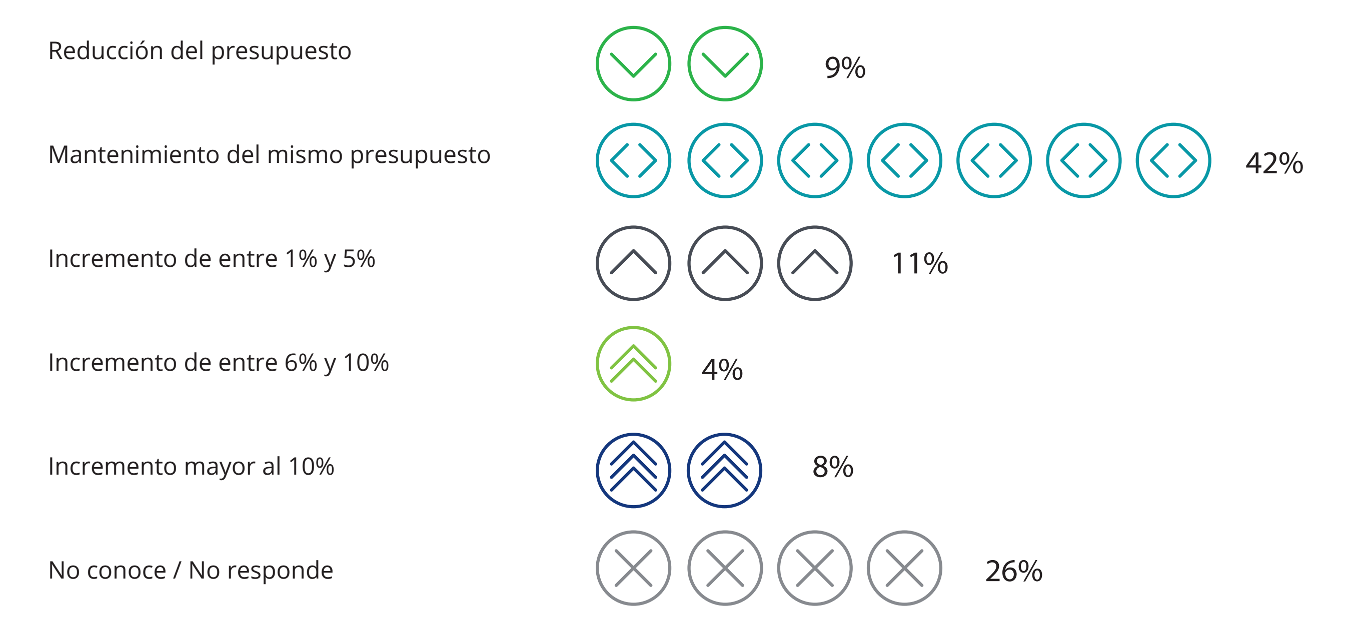


No, el presupuesto de SI está bajo otras funciones (ej. TI)

Contar con un presupuesto propio, administrado por el CISO, es un **paso fundamental para cumplir con una gestión efectiva** de la función de SI y apoyar en el cumplimiento de los objetivos del negocio.

Evolución del presupuesto

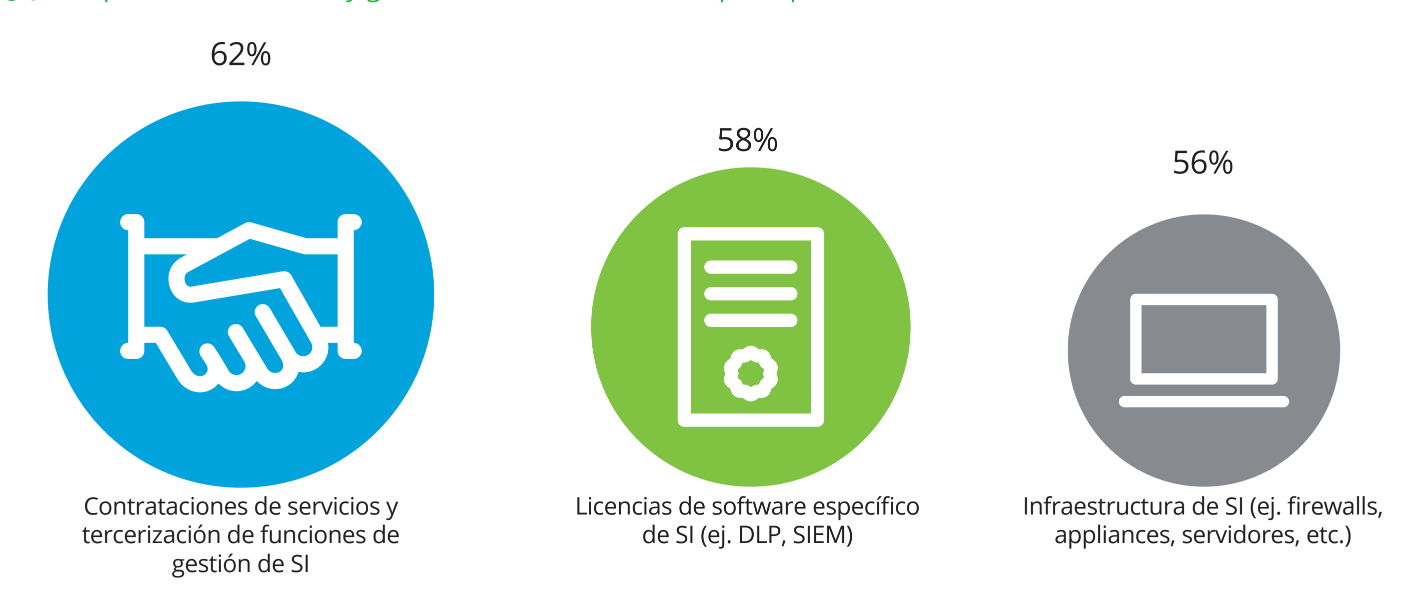
¿Cuál será la evolución del presupuesto de seguridad de información en 2018 en comparación con el presupuesto de 2017?



A pesar de la delicada situación a nivel país, **la mayoría de participantes han definido mantener su presupuesto** de seguridad para el próximo año. Esto podría obedecer a la creciente ola de ataques a nivel mundial y la ocurrencia de incidentes internos en las organizaciones.

Componentes del presupuesto

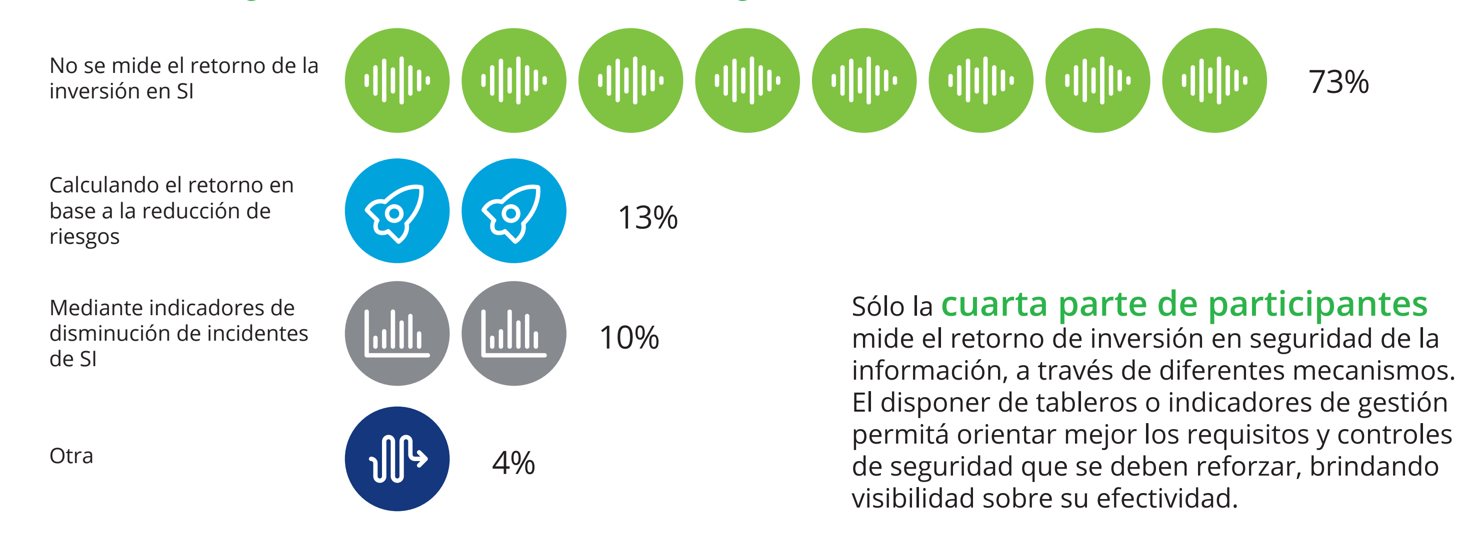
¿Qué aspectos, inversiones y gastos están incluidos en su presupuesto?



Los aspectos más importantes que se incluyen en el presupuesto son: la contración de servicios y tercerización de funciones de gestión de SI, adquisición de licencias de software e infraestructura tecnológica.

Retorno de inversión

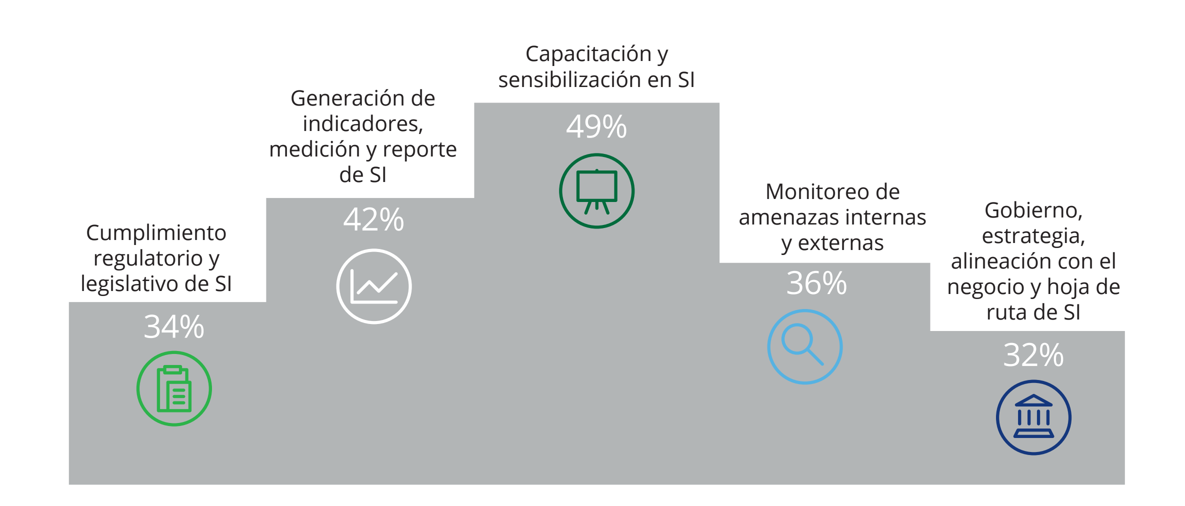
¿Cómo mide su organización el retorno de inversión en seguridad de la información?



Sólo la **cuarta parte de participantes** mide el retorno de inversión en seguridad de la información, a través de diferentes mecanismos. El disponer de tableros o indicadores de gestión permitá orientar mejor los requisitos y controles de seguridad que se deben reforzar, brindando visibilidad sobre su efectividad.

Principales iniciativas

Cinco principales iniciativas de seguridad de información para el año 2018



El **factor humano sigue siendo un aspecto prioritario** dentro de las iniciativas de seguridad de información para el 2018. Sin embargo, existen otras áreas que han ganado notoriedad para el siguiente año. Como parte de la evolución de seguridad de información, las organizaciones están reconociendo la importancia de indicadores que permitan determinar si se está cumpliendo con los objetivos propuestos así como la necesidad de mantener un enfoque proactivo frente a ataques a través del monitoreo de amenazas internas y externas.

Principal incentivo

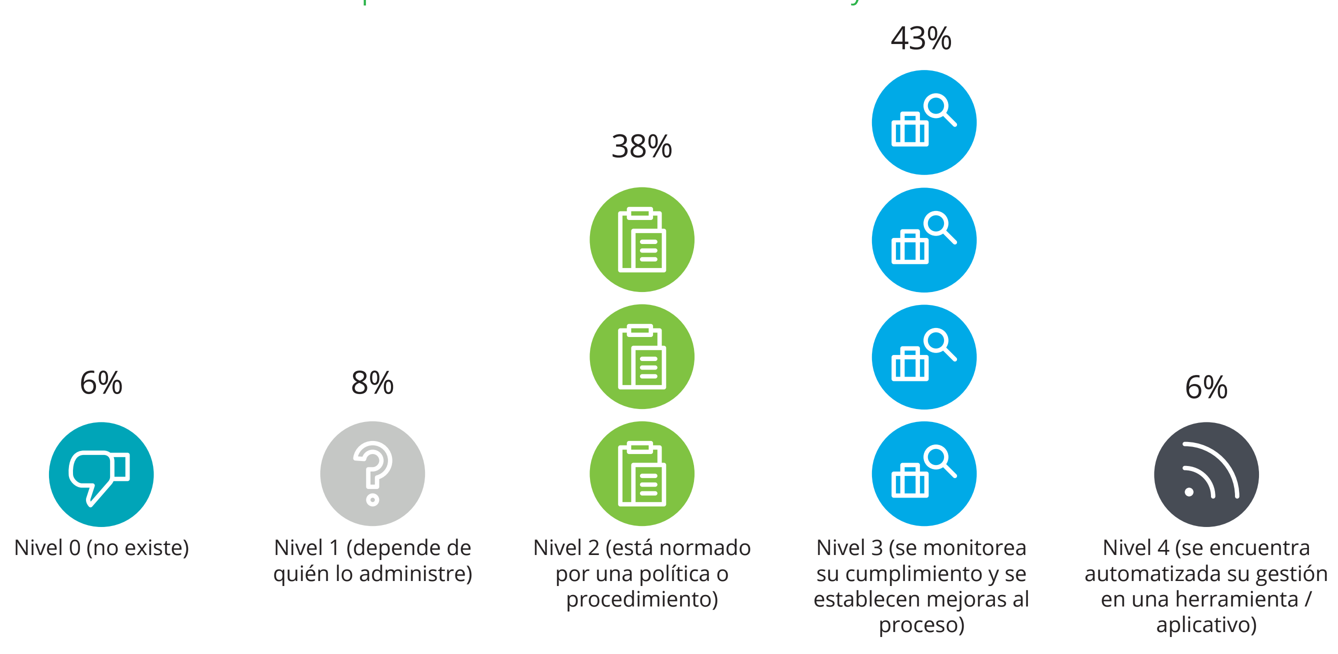
Identifique el principal incentivo que tiene el negocio para emprender iniciativas de seguridad de la información en su organización.



Si bien existen industrias donde la regulación presiona para invertir en seguridad de información, **3 de cada 4 participantes** consideran que los principales incentivos están asociados con el propio negocio y su necesidad de convertir a la seguridad en una herramienta habilitadora de procesos, productos y servicios más seguros, lo cual es clave para una buena gestión.

Nivel de madurez del proceso de administración

Califique el nivel de madurez de su proceso de administración de usuarios y accesos a recursos de información.



La administración de usuarios y accesos continúa siendo un proceso ejecutado y monitoreado manualmente, **por lo que es propenso a errores.** Implementar procesos automatizados y basados en herramientas constituye un aspecto prioritario y un reto en el camino de la madurez de este ámbito de la gestión de seguridad de información.

Adopción de tecnologías de seguridad

¿Cómo describe la adopción de las siguientes tecnologías en su organización?



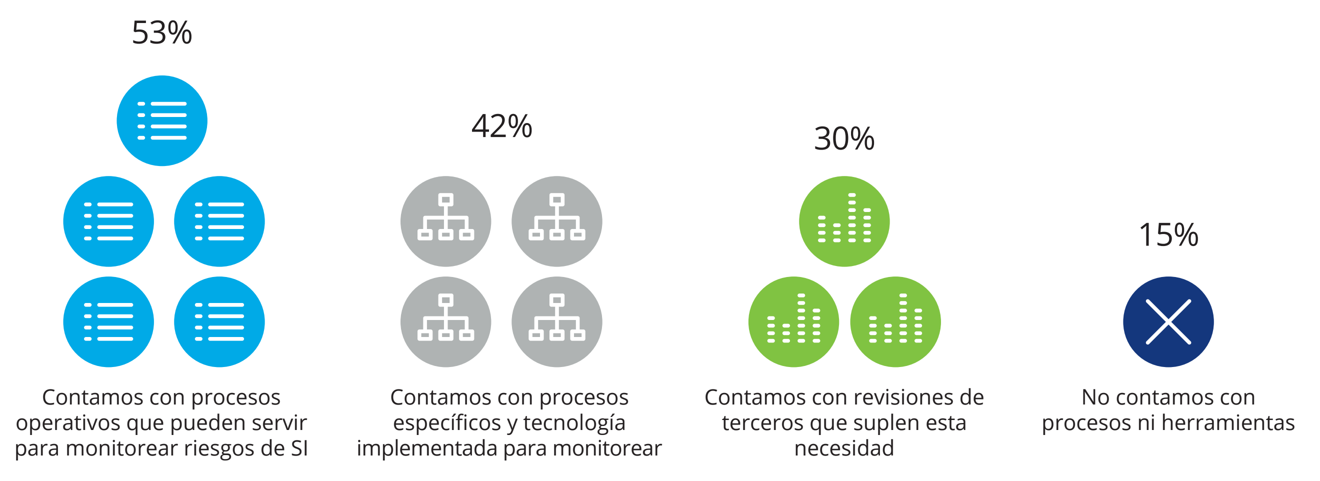
En el 2017 se evidencia un alto grado de conciencia de las amenazas y su gestión a través de la implementación de tecnologías principalmente en **seguridad perimetral.** El reto para el CISO será el implementar tecnologías que mitiguen las **amenazas emergentes** para el 2018.

Vigilante



Procesos y/o tecnologías de monitoreo de riesgos

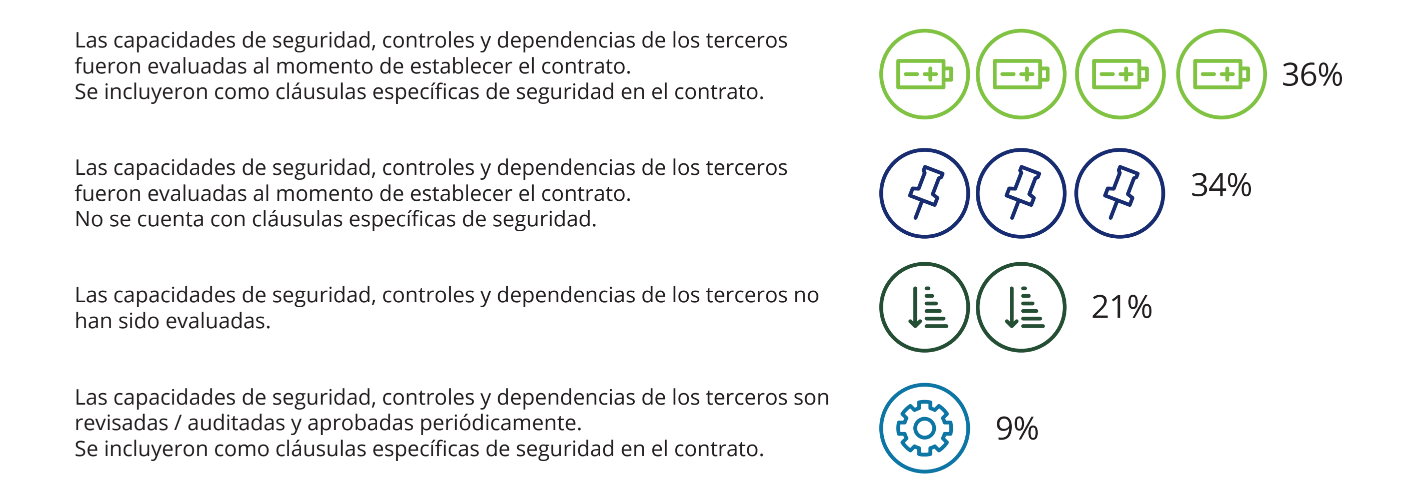
¿Qué procesos y/o tecnologías tiene implementados su organización para monitorear y evaluar los riesgos de seguridad de la información a los que está expuesta?



La mayoría de los participantes reconoce la importancia de monitorear riesgos de seguridad y actualmente cuenta con algún mecanismo para dicho efecto. Al mismo tiempo, **un tercio de los participantes** confían en revisiones realizadas por terceros pero que no tienen como foco la efectividad de la seguridad de información para la organización, lo cual nos permite concluir que existe aún espacio para su mejora.

Administración y monitoreo de la seguridad de terceros

¿Cómo administra y monitorea la seguridad de terceros con los cuales su organización hace negocio y/o terceriza parte de sus procesos de negocio?

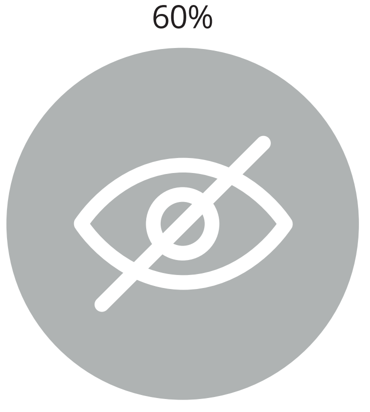


Los riesgos derivados de la exposición de la información empresarial con terceros han sido sujetos o han sido causantes de varios incidentes de seguridad en los últimos años. Casi la mitad de los participantes actualmente gestionan este tipo de riesgos, sin embargo **aproximadamente 2 de cada 5 empresas** aún no priorizan este tipo de riesgos como un aspecto clave de su gestión.

Centro de Operaciones de Seguridad (SOC)

¿Cuenta con un Centro de Operaciones de Seguridad (SOC)?

60%



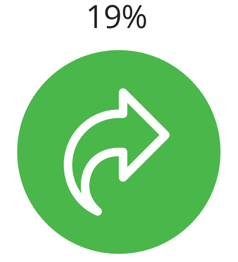
No disponemos de un Centro de Operaciones de Seguridad

21%



Si, contamos con un Centro de Operaciones de Seguridad

19%



No disponemos de un Centro de Operaciones de Seguridad pero pensamos implementar uno durante el año 2018

Contar con un SOC se ha convertido en un imperativo para la gestión de seguridad de la información, dado que reúne el personal y herramientas que realmente se necesitan para soportar la seguridad que la actividad del negocio requiere. Si bien más de la mitad de los participantes no disponen de un SOC, **1 de cada 5 participantes** consideran implementarlo para el 2018.

Capacidades del SOC

¿Qué capacidades tiene implementadas en el Centro de Operaciones de Seguridad (SOC)?

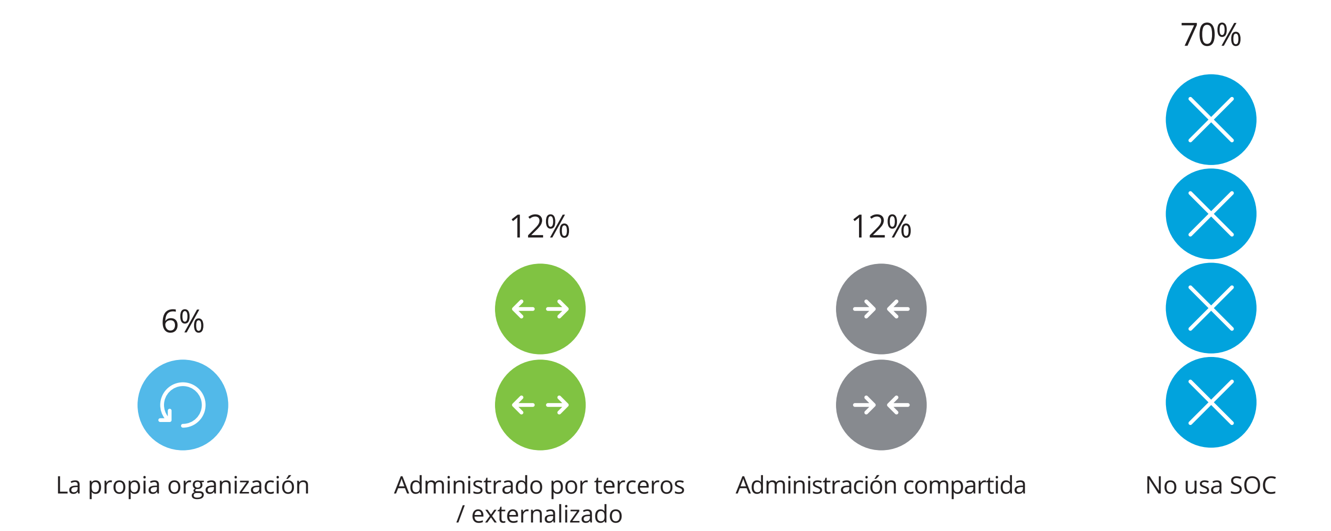


Monitoreo y correlación de eventos de seguridad (SIEM) | Monitoreo y gestión de amenazas | Respuesta para incidentes de seguridad | Administración de la seguridad | Monitoreo del tráfico y datos

Los servicios de SOC implementados en su gran mayoría **atacan los aspectos básicos del monitoreo de seguridad y respuesta a incidentes,** existiendo funciones de seguridad de la información por incorporar para optimizar y desarrollar dichos servicios.

Responsable del Centro de Operaciones de Seguridad

¿Quién es responsable por su Centro de Operaciones de Seguridad (SOC)?



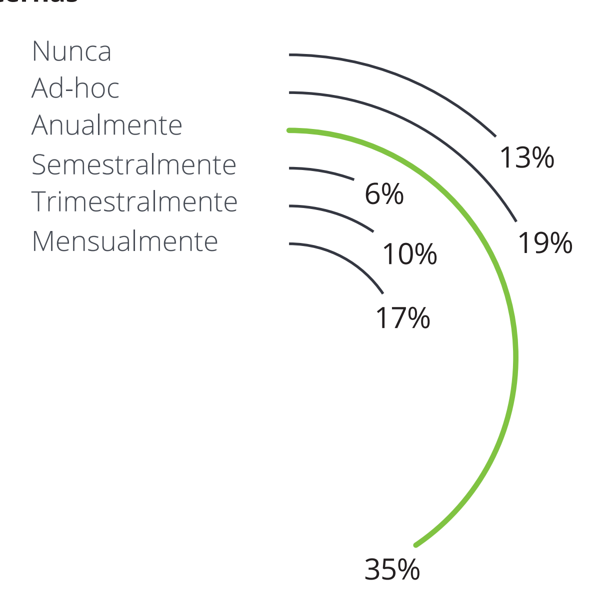
El **esquema de administración externalizado** sigue siendo atractivo para los participantes al momento de implementar un SOC debido al factor económico.

Frecuencia de evaluaciones de seguridad

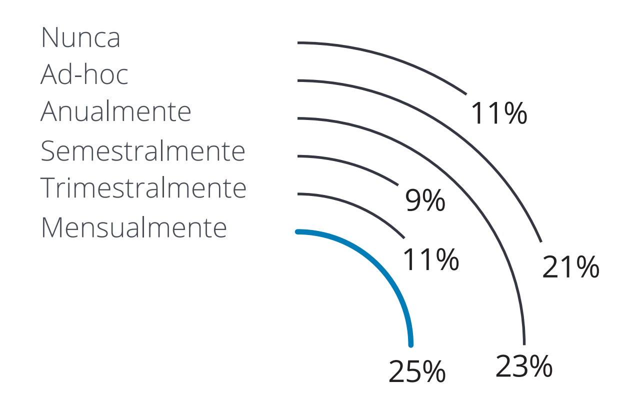
Indique con qué frecuencia realiza los siguientes procesos de evaluación / testeo de seguridad:

Existe una frecuencia definida a través de la cual se monitorean los riesgos de seguridad de la información para vulnerabilidades internas y externas y de aplicaciones web. Sin embargo, aún existe una brecha significiativa con las revisiones de código fuente considerando que existe una **marcada tendencia sobre la falta de aplicación de buenas prácticas de desarrollo seguro** tanto por las propias organizaciones como por terceros.

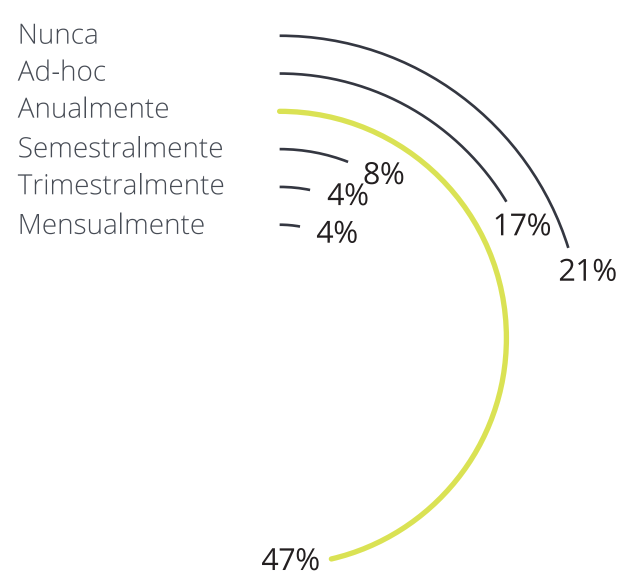
Escaneo de vulnerabilidades externas



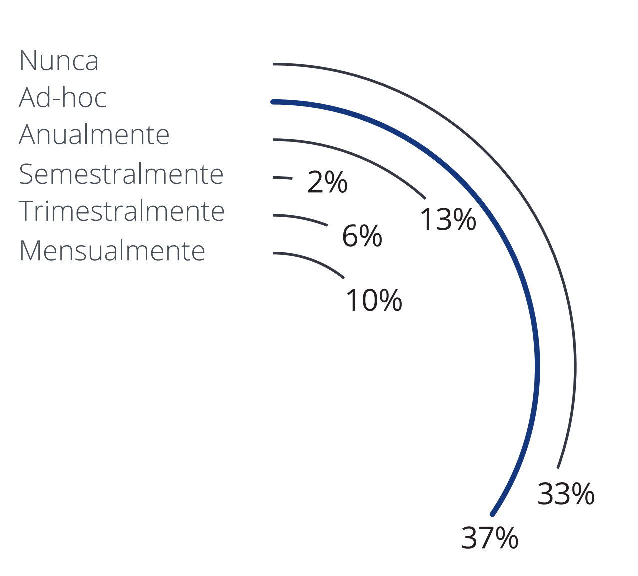
Escaneo de vulnerabilidades internas



Pruebas de penetración en aplicaciones web



Revisión de código fuente



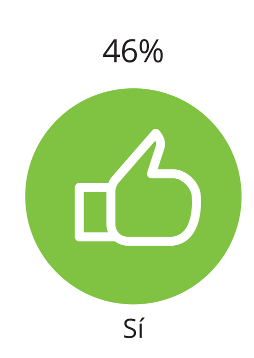
Resiliente



Brechas de seguridad interna y/o externa

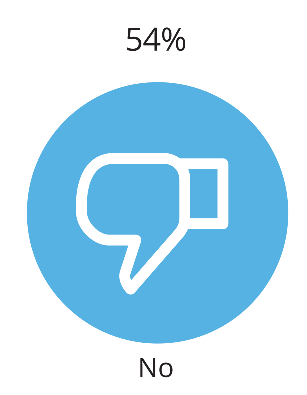
¿Su organización ha experimentado una brecha de seguridad interna y/o externa durante el último año?

46%



Sí

54%



No

Principales Brechas Externas

  28%

Software malicioso originado externamente

  21%

Pérdida o robo de equipos

 15%

Robo o pérdida de información.

Principales Brechas Internas

   22%

Robo de información causado por fallas en accesos de usuarios

  20%

Pérdida de equipos por descuido de empleados

 15%

Diseminación de software malicioso por desconocimento de empleados

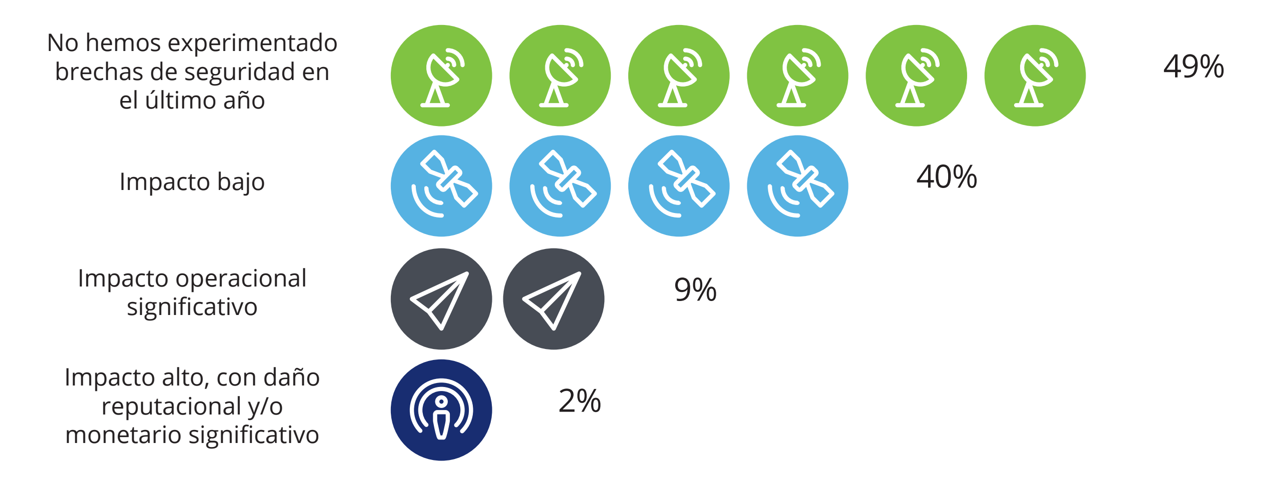
Casi la mitad de los participantes asegura que ha experimentado una brecha de seguridad interna y/o externa llevándolos a destinar más recursos, de tipo humano, económico y tecnológico, para la gestión efectiva de la seguridad de la información.

En el ámbito externo, el principal factor de riesgo es generado por el software malicioso, el cual ha sido responsable por notorios incidentes a escala mundial como el ransomware WannaCry.

Mientras que el ámbito interno, fallas o errores en el control interno (específicamente gestión de usuarios y accesos) han expuesto información empresarial a robos y/o pérdidas.

Impacto de las brechas de seguridad

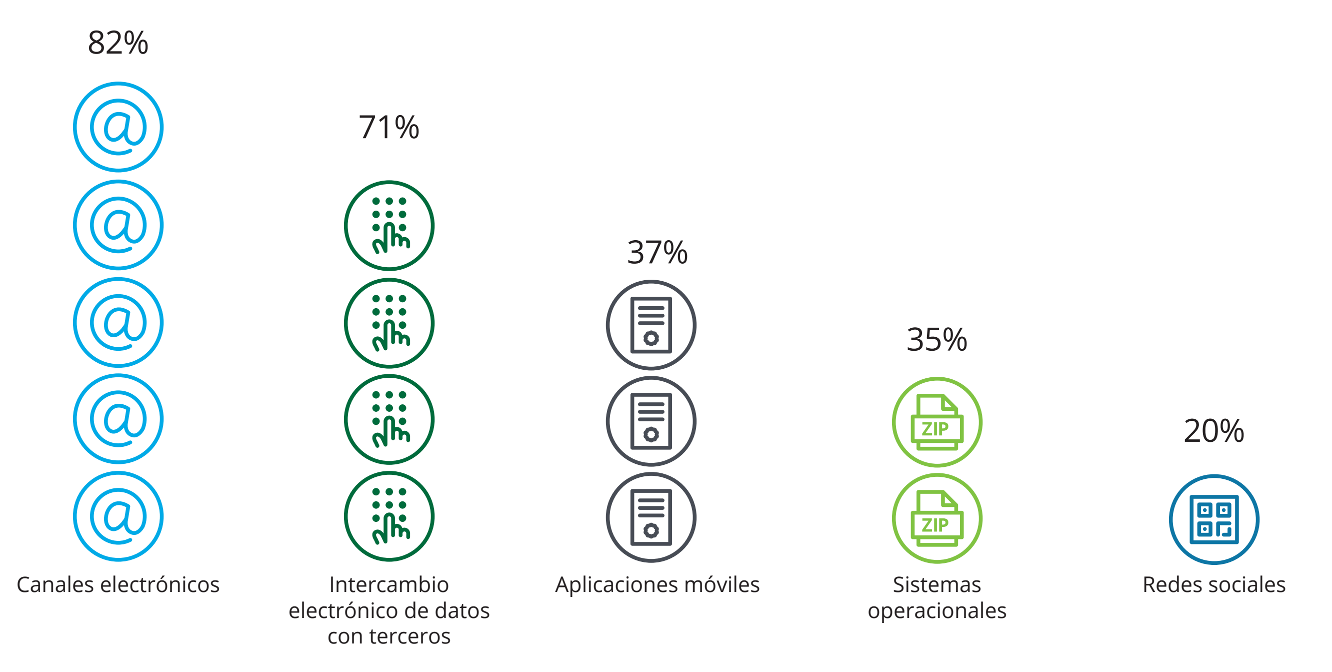
¿Cómo clasificaría la severidad/impacto de las brechas de seguridad sufridas por su organización en el último año?



1 de cada 10 participantes sufrieron brechas de seguridad significativas, y con pérdidas que llegaron hasta los USD 100,000. También se observa que **1 de cada 5 organizaciones** no puede determinar el impacto al no contar con mecanismos de registro y medición de incidentes.

Canales para gestionar la seguridad de la información

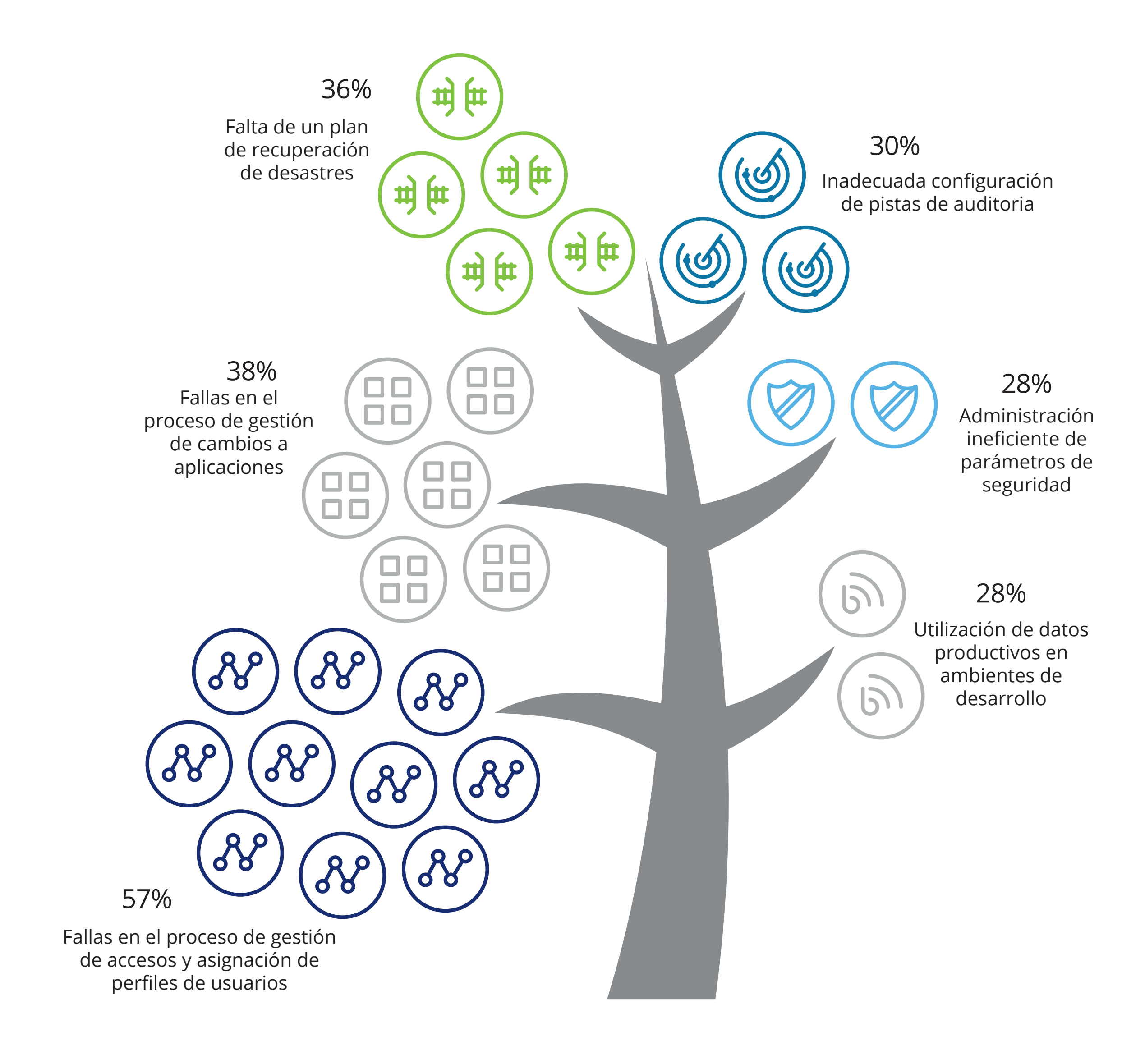
¿En qué áreas o en qué canales su organización se encuentra preparada para afrontar un incidente de seguridad de la información?



Las redes sociales son el canal que las empresas han encontrado para posicionar su marca e incrementar su participación de mercado. Sin embargo, **4 de cada 5 participantes** no gestionan los riesgos de seguridad resultantes de su uso en la organización.

Observaciones de auditoría interna o externa

Principales observaciones de auditoría, interna o externa, relacionados con seguridad de información en los últimos 12 meses.



Como producto de las diversas revisiones tanto externas como internas realizadas en las empresas, **la gestión de usuarios y accesos sigue siendo el elemento más tambaleante de la gestión de los CISOs.**

El uso de información de ambientes productivos sin los adecuados procesos de enmascaramiento y protección de datos sensibles, se encuentra como una de las principales observaciones de auditoría de este año, evidenciando la evolución de los alcances de auditoría como resultado de las nuevas amenazas de seguridad de la información.

Contactos

Oswaldo Bravo
Socio RA
(593 2) 381 5100 ext. 2224
obravo@deloitte.com

Roberth Chávez
Gerente Senior RA
(593 2) 381 5100 ext. 2119
rochavez@deloitte.com